



TITLE:

Fontaine-Mazur予想の紹介 (代数的整数論とその周辺)

AUTHOR(S):

田口, 雄一郎

CITATION:

田口, 雄一郎. Fontaine-Mazur予想の紹介 (代数的整数論とその周辺). 数理解析研究所講究録 1999, 1097: 37-49

ISSUE DATE:

1999-04

URL:

<http://hdl.handle.net/2433/63023>

RIGHT:

Fontaine-Mazur 予想の紹介

北大理 田口 雄一郎 (Yuichiro Taguchi)

Fontaine-Mazur 予想というのは、

既約かつ幾何学的な p 進 Galois 表現は代数幾何から来るであろう という主予想と、これから派生する様々な予想のことである。本稿ではこれらの予想といくつかの知られている結果 (特に不分岐 Fontaine-Mazur 予想 (§5)) について簡単に紹介する。§1 ~ §4 は通り一遍の解説になってしまった。詳しくは基本文献 [19] 及び [17] を参照されたい。また §5 の内容については、山岸氏の論説 [43] も合せて御覧下さい。

議論につき合っているいろいろ御教示下さった斎藤毅さん、志甫淳さん、予想 M についての質問に答えて下さった B. Mazur さん、函数体の不分岐拡大についての御注意及び御説明を下さった伊原康隆先生、貴重な文献をお送り下さった山岸正和さん、山村健さん、R. Taylor さんに感謝します。

* * *

まずは「大風呂敷」¹ の話から始めよう。次の問題を考える：

問題. Galois 表現を分類せよ。

即ち、 K を体として、集合

$$\mathfrak{X} = \{ \rho : G_K \rightarrow \mathrm{GL}(V); \cdots (\text{条件}) \cdots \} / \text{同型}$$

を考える。ここで $G_K = \mathrm{Gal}(\overline{K}/K)$ は K の絶対 Galois 群、 $\mathrm{GL}(V)$ は線型空間 V の自己同型群である。べつに線型表現にこだわらずに、 ρ の行き先として、例えば $\mathrm{Aut}(\text{基本群})$ の様なものをも考えることもできるだろうし、 G_K より「調べ易い」群なら何でもよいわけである。

さて「分類する」というとき我々はだいたい次の様なことを考える：

A. 集合 \mathfrak{X} を決定せよ。

(1) 有限か無限か？

(2) 特に、空でないか？

— 例えば、与えられた有限群 G に対し $\mathfrak{X} = \{ \text{全射 } \rho : G_K \rightarrow G \}$ が空でないか？
 というのは有名な Galois の逆問題である。

(3) \mathfrak{X} は何らかの構造を持つか？ 持つならばそれはどんなものか？

— 例えば Mazur の「Galois 表現の変形理論」はこれの一例と言えよう。

(4) $\rho \in \mathfrak{X}$ と他の (よりわかり易い) 対象との対応。

— 例えば Fontaine の「filtered module の理論」はこれの一例と言えよう。

B. 各 $\rho \in \mathfrak{X}$ を (なるべく具体的に) 構成せよ。例えば：

(1) 解析函数の特殊値を使って (Hilbert の第 12 問題)。

¹ 「風呂敷」の語源のほうにむしろ興味を示してくださった人もいたので、一応責任上『広辞苑』を引いてみると：(1) 風呂に入る時には衣類を包んでおき、湯からあがった時には足を拭うのに用いた布。一代女_五「ゆふべゆふべのぬれ景色、座をとつて—の上に直れば」(2) 物を包むのに用いる方形の布。古くは「ひらづつみ」ともいう。「—包み」… (後略) とのことです。

(2) Modular form から。

(3) Etale cohomology 群 $H_{\text{ét}}^i(X_{\bar{K}}, \mathbb{Q}_p(r))$ や代数的基本群 $\pi_1(X_{\bar{K}})$ として。

Fontaine-Mazur 予想は、 K を有限次代数体として、 $\mathfrak{X} = \{\rho : G_K \rightarrow \text{GL}_n(\mathbb{Q}_p); \text{既約かつ幾何学的}\}$ に対して、上の **A** のような諸問題や、また、**B** の (3) の様な問題を考えるものである。

以下 K は有限次代数体とし、 $G_K := \text{Gal}(\bar{K}/K)$ とおく。また E を p 進体 \mathbb{Q}_p の有限次拡大とし、連続 E -線型表現 $\rho : G_K \rightarrow \text{GL}_E(V)$ を考える (V は有限次元 E -線型空間)。(K は“基礎体”、 E は“係数体”である。)

1. 主予想. 言葉の説明は後にして、まづ予想を述べてしまおう：

予想 G. 既約かつ幾何学的な表現

$$\rho : G_K \rightarrow \text{GL}_E(V)$$

は代数幾何から来るであろう。

注意. この逆 (代数幾何から来る表現は幾何学的) は、永いこと何となく予想されていたことだと思うが、今では辻氏 (+ de Jong) の定理 [40] である。

問. 既約でないときはどう定式化したらいだろうか。(代数幾何から来る表現を二つ持って来て勝手に拡大を作ると、必ずしも代数幾何から来るものにはならない。 p 進表現としての Ext は \mathbb{Q}_p -線型空間だが、その中で代数幾何から来るものは特別な \mathbb{Q} -線型空間をなすはずである。)

定義. (「幾何学的」というのは係数体 E によらない条件なので、 \mathbb{Q}_p -線型表現 $\rho : G_K \rightarrow \text{GL}_{\mathbb{Q}_p}(V)$ について述べる。) ρ が幾何学的とは次が成立つこと：

- (1) ρ は有限個の素点を除き不分岐；
- (2) K の全ての素点 v に対し ρ の v への制限

$$\rho_v : G_{K_v} \rightarrow \text{GL}_{\mathbb{Q}_p}(V)$$

は potentially semi-stable.

ここで K_v は K の v での完備化であり、 $G_{K_v} = \text{Gal}(\bar{K}_v/K)$ は $\bar{K} \hookrightarrow \bar{K}_v$ により v の惰性群 $\subset G_K$ と同一視する。

また、 $\rho_v : G_{K_v} \rightarrow \text{GL}_{\mathbb{Q}_p}(V)$ が potentially semi-stable とは

(1) ($v|p$ のとき) ある開部分群 $H \subset I_v$ に対し $\dim_{\mathbb{Q}_p'}(B_{\text{st}} \otimes V)^H = \dim_{\mathbb{Q}_p} V$ となること (ここに \mathbb{Q}_p' は \mathbb{Q}_p の最大不分岐拡大の p 進完備化)；

(2) ($v \nmid p$ のとき) ある開部分群 $H \subset I_v$ があって、 H は V に冪単 (unipotent) に作用すること、である。

注意. $v \nmid p$ のとき、任意の p 進表現 $\rho_v : G_{K_v} \rightarrow \text{GL}_{\mathbb{Q}_p}(V)$ は potentially semi-stable であることが知られている (Grothendieck の定理 — cf. [37] の附録)。

定義. $\rho : G_K \rightarrow \text{GL}_E(V)$ が代数幾何から来るとは、ある (射影的かつ滑らかな) K 上の代数多様体 X があって、 ρ が $E \otimes_{\mathbb{Q}_p} H_{\text{ét}}^i(X_{\bar{K}}, \mathbb{Q}_p(r))$ のある部分商として実現されることである (ここに $X_{\bar{K}} := X \otimes_K \bar{K}$)。

注意. “射影的かつ滑らか” は、特異点解消を使うと、仮定してもしなくても同じことになる。

上の予想よりもさらに強く、次が期待されている：

期待 H. 任意の幾何学的表現は Hecke 的である。

ここで、表現 $\rho: G_K \rightarrow \mathrm{GL}_E(V)$ が Hecke 的 とは、ある保型表現上の “Hecke 作用素” T_v (v は K の素点) たちにより生成されるある有限型 \mathbb{Z}_p -代数 \mathcal{H} と、ある \mathcal{H} 上の連続表現 $\tilde{\rho}: G_K \rightarrow \mathrm{GL}_n(\mathcal{H})$ とがあつて、 ρ は $\tilde{\rho}$ からある \mathbb{Z}_p -代数射 $f: \mathcal{H} \rightarrow E$ により得られ、しかも $\mathrm{Trace}(\rho(\mathrm{Frob}_v)) = f(T_v)$ となっていることを言う。

2. 有限性予想. 一般に次の様な記号を使う：

$$\mathrm{Rep}_E(G)^{\text{条件}} := \{ \text{表現 } \rho: G \rightarrow \mathrm{GL}_E(V); \dots(\text{条件})\dots \} / \text{同型},$$

$$G_{K,S} := \mathrm{Gal}(S \text{ の外不分岐最大拡大 } / K)$$

ここに S は代数体 K の素点の有限集合である。

予想 F(a) 任意の inertial level \mathcal{L} と任意の $\overline{\mathbb{Q}}_p$ -Hodge-Tate 型 h に対し、集合 $\mathrm{Rep}_{\overline{\mathbb{Q}}_p}(G_{K,S})^{\mathrm{geom}, \mathcal{L}, h}$ は有限であろう。

(b) 任意の inertial level \mathcal{L} と任意の E -Hodge-Tate 型 h に対し、集合 $\mathrm{Rep}_E(G_{K,S})^{\mathrm{geom}, \mathcal{L}, h}$ は有限であろう。

(c) 任意の E -Hodge-Tate 型 h に対し、集合 $\mathrm{Rep}_E(G_{K,S})^{\mathrm{geom}, h}$ は有限であろう (i.e. 係数体 E が有限次 $/\mathbb{Q}_p$ なら inertial level \mathcal{L} は止めなくてもよい)。

ここに inertial level とは (potentially semi-stable 表現 ρ は K を有限次拡大で取り換えると semi-stable になるわけだが) K をどれくらい分岐させれば semi-stable になるか、というその level で、正確に言うとは：

定義. Inertial level $\mathcal{L} = (\mathcal{L}_v)_{v \in S}$ とは、惰性群 I_v の開正規部分群 \mathcal{L}_v の族 (for $v \in S$) のこと。 $G_{K,S}$ の表現 ρ が inertial level \mathcal{L} である とは、全ての $v \in S$ に対し ρ の \mathcal{L}_v への制限 $\rho|_{\mathcal{L}_v}$ が semi-stable であること。

また、

定義. $\rho: G_K \rightarrow \mathrm{GL}_E(V)$ の、素点 $v|p$ での E -Hodge-Tate 型 h_v とは、次数付 $(E \otimes_{\mathbb{Q}_p} K_v)$ -加群 $D_{\mathrm{HT}}^*(V) = \mathrm{Hom}_{\mathbb{Q}_p[G_{K_v}]}(V, B_{\mathrm{HT}, v})$ の同型類のこと。単に E -Hodge-Tate 型 と言ったら $h = (h_v)_{v|p}$ のこと。 E の代わりに $\overline{\mathbb{Q}}_p$ の場合も同様。

注意. 上の三つの予想の間の論理的関係は：

$$(a) \Rightarrow (b) \Leftrightarrow (c)$$

となっている ((a) \Rightarrow (b) \Leftarrow (c) は à priori に成り立つが、(b) \Rightarrow (c) は少し考える必要あり)。

注意. $\mathrm{Rep}_{\overline{\mathbb{Q}}_p}(G_{K,S})^{\mathrm{geom}, h}$ は無限集合になる (e.g. $\chi_n: G_{\mathbb{Q}, \{p, \infty\}} \rightarrow \mathrm{Aut}(1 \text{ の } p^n \text{ 乗根}), n = 1, 2, \dots$)。

例. (a) Abrashkin, Fontaine の結果 ([1], [16]): $K = \mathbb{Q}$ 及びいくつかの二次体, $S = \{ \text{小さい素数 } p, \infty \}$ のとき、特別な形の Hodge-Tate 型を持つ crystalline 表現は存在しないことが言える。これは予想 F(a) の状況証拠になっている。

(c) Faltings [15] により証明された Shafarevich 予想 (S の外で good reduction な g 次元主偏極 Abel 多様体は有限個) は、予想 F(c) の状況証拠になっている;

$$(\text{Abel 多様体から来るもの}) \cap \text{Rep}_E(G_{K,S})^h = \text{有限}$$

(この場合、 S での inertial level は止めなくてよい)。

ところで、上の様な有限性予想に (直接論理的関係は無いが) なんとなく関連がありそうな問題として、次の様な問題が考えられる (cf. [33]): 連続表現

$$\rho: G_{\mathbb{Q}} \rightarrow \text{GL}_n(\overline{\mathbb{F}}_p)$$

に対し、 $N(\rho)$ をその「Artin conductor の p と素な部分」(cf. [36], §1.2) とする。

問題. 与えられた自然数 N に対し、 $N(\rho)|N$ なる連続表現 $\rho: G_{\mathbb{Q}} \rightarrow \text{GL}_n(\overline{\mathbb{F}}_p)$ の同型類の個数は有限個か?

$n=1$ の場合は類体論により OK, $n=2$ の場合は、Serre の予想 [36] を認めると「odd かつ既約」の場合は OK である (また、 $N=1$ で p が小さいとき、Tate の結果 [39] がある)。 $n=4$ 乃至 8 で $p=2, 3$, $N=1$ の場合には文氏の部分的結果 [33] がある。

3. 保型性予想 (= 期待 H の elliptic modular case).

予想 M. $\rho: G_{\mathbb{Q}} \rightarrow \text{GL}_{\overline{\mathbb{Q}}_p}(V)$ は $G_{\mathbb{Q}}$ の 2 次元既約幾何学的 $\overline{\mathbb{Q}}_p$ -表現であり、Artin 表現 (i.e. 像が有限な表現) の Tate 捻りではない、と仮定する。このとき、ある $i \in \mathbb{Z}$ に対し V の Tate 捻り $V(-i)$ は modular, 即ちある newform f に伴う表現と同型 (或いは L -函数の言葉で、 $L(V(-i), s) = L(f, s)$) となるであろう。

これはもちろん谷山-志村-Weil 予想の一般化である。この予想から、特に、有限性予想 F(a) の、 $K = \mathbb{Q}$, $\dim_{\overline{\mathbb{Q}}_p} V = 2$ の場合が従う (\mathcal{L} と h を固定することは保型形式 f の level N と重さ k を固定することに対応する)。

注意(Mazur 氏の email による). この予想には、その一部として「Artin 表現の Tate 捻りでない 2 次元既約幾何学的表現は自動的に odd (i.e. $\det \rho$ (複素共役) $= -1$) であろう」ということが含まれているらしい。Artin 表現の Tate 捻りの場合は odd か even かの区別は厳しく、odd なら重さ 1 の保型形式から来るとされるわけだが、even な表現も “really fascinating” とのことである。

さてこの予想に関して、Wiles [42] 以降もいろいろ発展があるが、それらは他でも解説されていると思うので略して、一つだけ \mathbb{Q} 上の楕円曲線の場合の比較的新しい結果を挙げると、Conrad-Diamond-Taylor による次の結果がある:

定理 ([11]). \mathbb{Q} 上の楕円曲線 E の導手が 3^3 で割れないならば E は modular.

Wiles の場合の flat deformation の代りに、より一般的な potentially Barsotti-Tate deformation を使うのがポイントのようだ。

4. 変形理論. これまで述べてきた予想は Galois 表現の普遍変形環の言葉で再定式化しておくとも便利である。

記号：

\mathcal{O}_E : E の整数環

k : E の剰余体

\mathcal{C} : 完備 Noether 局所 \mathcal{O}_E -代数であって剰余体 $= k$ なるもののなす圏
(ただし射は剰余体上 id_k なるもの)

$G = G_{K,S}$ or G_{K_v}

$\underline{\text{Rep}}_A(G)^{\text{条件}}$: A 上有限型な $A[G]$ -加群であって「条件」を満たすもののなす圏

定義. 表現 $\bar{\rho}: G \rightarrow \text{GL}_n(k)$ の $A \in \mathcal{C}$ への変形 (deformation) とは、可換図式

$$\begin{array}{ccc} G & \xrightarrow{\rho} & \text{GL}_n(A) \\ \bar{\rho} \searrow & & \downarrow \text{mod } \mathfrak{m}_A \\ & & \text{GL}_n(k) \end{array}$$

のこと。ただし $U \equiv 1_n \pmod{\mathfrak{m}_A}$ なる行列 U により共役な ρ たちは同一視する。

Wiles は「変形の型」 \mathcal{D} (e.g. $\mathcal{D} = (\text{ord}, S, \mathcal{O}, \mathcal{M})$ など) というものを考えたが、Fontaine, Mazur らは、一般に、長さ有限 $\mathcal{O}_E[G]$ -加群の圏 $\underline{\text{Rep}}_{\mathcal{O}_E}^{\text{fin}}(G)$ の任意の部分圏 \mathcal{D} であって、部分、商、直和を取る操作について閉じているもの、に対し「 \mathcal{D} -型の変形」を考えるべきだとしている (cf. [17] または [31] の §23 Deformation conditions) (とは言っても、いくつかの特別な \mathcal{D} だけが重要なのだが)。即ち、

$$\bar{\rho} \in \underline{\text{Rep}}_k(G) \cap \mathcal{D}$$

に対し、函手

$$\begin{aligned} F_{\bar{\rho}, \mathcal{D}}: \mathcal{C} &\rightarrow (\text{Sets}) \\ A &\mapsto \{\bar{\rho} \text{ の変形 in } \underline{\text{Rep}}_A^{\mathcal{D}}(G)\} \end{aligned}$$

を考える。ここに $\underline{\text{Rep}}_A^{\mathcal{D}}(G)$ は $U \in \underline{\text{Rep}}_A(G)$ であってその全ての有限商が \mathcal{D} に入るもののなす圏。もちろん「条件無し」(i.e. $\mathcal{D} = \underline{\text{Rep}}_{\mathcal{O}_E}^{\text{fin}}(G)$ の場合) の函手

$$\begin{aligned} F_{\bar{\rho}}: \mathcal{C} &\rightarrow (\text{Sets}) \\ A &\mapsto \{\bar{\rho} \text{ の変形 in } \underline{\text{Rep}}_A(G)\} \end{aligned}$$

も考えられる。

命題 ([30], [13] etc.) もし $H^0(G, \text{End}(\bar{\rho})) = k$ ならば、函手 $F_{\bar{\rho}, \mathcal{D}}$ は表現可能である。即ち、普遍変形環 $R(\bar{\rho})_{\mathcal{D}}$ (in \mathcal{C}) と普遍変形 $\rho_{\mathcal{D}}^{\text{univ}}: G \rightarrow \text{GL}_n(R(\bar{\rho})_{\mathcal{D}})$ とが存在して、 $\bar{\rho}$ の任意の変形 $\rho: G \rightarrow \text{GL}_n(A)$ の同型類はある unique な射 $f: R(\bar{\rho})_{\mathcal{D}} \rightarrow A$ により

$$\begin{array}{ccc} G & \xrightarrow{\rho_{\mathcal{D}}^{\text{univ}}} & \text{GL}_n(R(\bar{\rho})_{\mathcal{D}}) \\ \rho \searrow & & \downarrow \text{GL}_n(f) \\ & & \text{GL}_n(A) \end{array}$$

として得られる。さらに $H^1(G, \text{End}(\bar{\rho}))$ が有限次元ならば $R(\bar{\rho})_{\mathcal{D}}$ は noetherian である。

さて、Wiles の示したことは

V が “ある種の” Hecke 的 2 次元 E -表現ならば、
それに “十分近い” 幾何学的 E -表現はみな Hecke 的である

ということだったと言えよう。Fontaine と Mazur は、この “ある種の” を、一般に上の様な部分圏 $\mathcal{D} \subset \underline{\text{Rep}}_{\mathcal{O}_E}^{\text{fin}}(G_{K,S})$ のこと、として、“十分近い” を次の様に定義する ([17]):

定義. $\underline{\text{Rep}}_E^{\mathcal{D}}(G)$ を、 $V \in \underline{\text{Rep}}_E(G)$ であって $U \in \underline{\text{Rep}}_{\mathcal{O}_E}^{\mathcal{D}}(G)$ となる lattice $U \subset V$ が存在する様なものたちのなす圏、とする (ここ及び以下で V の lattice U とは K 上 V を張る部分 \mathcal{O}_E -加群で G -安定なものとする)。

$V \in \underline{\text{Rep}}_E^{\mathcal{D}}(G_{K,S})$ とし、 U を V の一つの lattice とする。 $u := U/\pi U$ (π は E の素元) は $G_{K,S}$ の表現として絶対既約であるとする (一つの U でそうならば他の lattice でもそうなる)。このとき $V' \in \underline{\text{Rep}}_E(G_K)$ が \mathcal{D} -close to V であるとは、

- (1) ある lattice $U' \subset V'$ があって $U'/\pi U' \simeq u$;
- (2) $V' \in \underline{\text{Rep}}_E^{\mathcal{D}}(G_{K,S})$

であること。

ところで特に重要と思われる部分圏 \mathcal{D} として次の様なものが考えられる:

$$\mathcal{D}_{\text{crys}} = \underline{\text{Rep}}_{\mathcal{O}_E}^{\text{fin}}(G_{K,S})^{\text{crys}, \mathcal{L}, h}, \quad \mathcal{D}_{\text{geom}} = \underline{\text{Rep}}_{\mathcal{O}_E}^{\text{fin}}(G_{K,S})^{\text{geom}, \mathcal{L}, h}.$$

即ち (inertial level と Hodge-Tate 型を固定した上で) potentially crystalline 表現や potentially semi-stable 表現の部分商として現れ得る長さ有限 $\mathcal{O}_E[G_{K,S}]$ -加群のなす圏である。すると先の予想は例えば次の様に表現できる:

予想 $F_{\mathcal{D}}$. 普遍変形環 $R(\bar{\rho})_{\mathcal{D}_{\text{geom}}}$ は \mathcal{O}_E -代数として有限であろう。

ちなみに 2 次元表現のとき、大雑把に言うと、局所的な $\bar{\rho}_v: G_{K_v} \rightarrow \text{GL}_2(k)$ の普遍変形環は \mathcal{O}_E 上だいたい 5 次元であり、このうち「大域に延びるもの」が 3 次元分、「幾何学的なもの」が 2 次元分で、これらが “transversal” に交ってくれているとすると、大域的かつ幾何学的な $R(\bar{\rho})_{\mathcal{D}_{\text{geom}}}$ は \mathcal{O}_E 上有限、という感じになっている様である (cf. [19] の Introduction).

また、

期待 $H_{\mathcal{D}}$. 普遍変形環 $R(\bar{\rho})_{\mathcal{D}_{\text{geom}}}$ はある保型表現上の Hecke 環の完備化として得られるであろう。

圏 $\mathcal{D}_{\text{crys}}$ は適当な条件の下ではある種の filtered modules の圏と同値になる ([18]). また $\mathcal{D}_{\text{geom}}$ に対応する filtered modules の圏を定義しようという試みは都築氏や坂内氏らによりなされていたが、最近では Breuil ([4]) がある種の $\widehat{W}\langle u \rangle$ -加群の圏としてよい圏を作っているようだ。このように \mathcal{D} を filtered modules の圏 $\text{MF}^{\mathcal{D}}$ として構成する利点は、

$$H_{\mathcal{D}}^1(G_{K_v}, \text{End}(U/\pi^n U))$$

などの重要な群が

$$\text{Ext}_{\text{MF}^{\mathcal{D}}}^1(M_n, M_n)$$

(ここに M_n は $U/\pi^n U$ に対応する filtered module) として比較的容易に計算できる (かもしれない) ということにある。

例えば $\bar{\rho} : G_{\mathbb{Q}_p} \rightarrow \mathrm{GL}_2(\mathbb{F}_p)$ の変形理論はよくわかっていて ([19], Chap. II), その普遍 crystalline (resp. potentially Barsotti-Tate) 変形は pst-module (filtered module の一種) の族として explicit に書けている。これは [10] で有効に使われている (はず)。

ここで参考までに Gouvêa の予想について簡単にふれておこう。

$$\bar{\rho} : G_{\mathbb{Q},S} \rightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_p), \quad \text{odd かつ既約}$$

とする。さらにこれが modular と仮定しよう; $\bar{\rho} = \bar{\rho}_f$ (Serre の予想 [36])。このとき Gouvêa は、だいたい

$$(\bar{\rho} \text{ の変形}) \leftrightarrow (f \text{ の変形 ; Katz の意味の } p \text{ 進 modular eigenform として})$$

であろう、と予想している ([21])。これの “部分” として

$$(\text{幾何学的変形}) \leftrightarrow (\text{古典的 modular eigenforms})$$

となっているはずである (cf. 予想 M)。

Gouvêa と Mazur ([22]) は $\bar{\rho} : G_{\mathbb{Q},\{p,\infty\}} \rightarrow \mathrm{GL}_2(\mathbb{F}_p)$ が modular で適当な条件 (level = p , 重さ k で、non-critical, i.e. U_p -作用素の slope $\neq 0, k-1$) をみたすときに、上段の \leftrightarrow に相当する事実を示している。ここで鍵として使われるのが Coleman の定理 ([7], [8]) で、古典的な eigenform が overconvergent p 進 modular eigenform の 1-parameter family (parametrized by k) に延びる、というもの (肥田理論の一部の一般化) である。これにより、変形空間の中に「modular な点」が一つあると、そこを通る「modular な曲線」が描ける。さらに non-critical なら companion form (又は twin; cf. [23]) の存在により、そこで交わる二本の曲線が描ける。これらの曲線上の $k \in \mathbb{Z}$ なる点でこの操作が出来るから、各曲線に無限個の曲線が交ったものが無限に続く様な絵が画ける。Mazur はこれを “infinite fern” と名付けた ([32], fern とは羊歯の謂)。今の場合 $R(\bar{\rho}) \simeq \mathbb{Z}_p[[T_1, T_2, T_3]]$ で、上の羊歯が 1 次元、その各点を指標で捻ることにより計 2 次元分が得られる。あと 1 次元分努力して、[22] の定理が得られる。

なお、上の羊歯の絵は Coleman-Mazur ([9]) により “eigencurve” なるものに一般化されている。

5. 不分岐予想. この節では S は p と素 (i.e. 全ての $v \in S$ に対し $v \nmid p$) なる場合を考察する。このとき $\rho : G_{K,S} \rightarrow \mathrm{GL}_n(\mathbb{Q}_p)$ は p で不分岐だから、特に p での Hodge-Tate weights = 0 である。そこで ρ が幾何学的であるとして (既約でなくてもよい) 予想 G と代数的サイクルについての標準的な予想を認めると、 ρ は代数的サイクルで張られる \mathbb{Q} -線型空間上実現されることになる。特にその像は有限である：

予想 UR^{geom}. S が p と素ならば $G_{K,S}$ の任意の幾何学的 p 進表現 $\rho : G_{K,S} \rightarrow \mathrm{GL}_n(\mathbb{Q}_p)$ は $G_{K,S}$ のある有限商を経由するであろう。

さらに Grothendieck の定理により $\rho : G_{K,S} \rightarrow \mathrm{GL}_n(\mathbb{Q}_p)$ は自動的に potentially semi-stable なので、「幾何学的」という条件は実は不要である；即ち上は次と同値：

予想 UR. S が p と素ならば $G_{K,S}$ の任意の p 進表現 $\rho : G_{K,S} \rightarrow \mathrm{GL}_n(\mathbb{Q}_p)$ は $G_{K,S}$ のある有限商を経由するであろう。

p 進解析的群は (ある n に対する) $\mathrm{GL}_n(\mathbb{Q}_p)$ のある部分群と同型であるから、上の予想は次の様に言っても同じ：

予想 UR'. S が p と素ならば $G_{K,S}$ の任意の p 進解析的商は有限であろう。

また、 p 進解析的群は p -uniform な指数有限部分群を含む (cf. 下の定義と注意) から、全ての K, S に対する予想 UR' は全ての K, S に対する次の予想と同値：

予想 UR''. S が p と素ならば $G_{K,S}$ の任意の p -uniform な商は有限であろう。

ここに

定義. Pro- p 群 G が p -uniform とは、ある filtration $G = G_1 \supset G_2 \supset \cdots$ (G_i は G の開部分群) であって

$$(*) \quad \bigcap_i G_i = 1, \quad G_i/G_{i+1} \text{ は abelian,} \quad p \text{ 乗} : G_{i-1}/G_i \xrightarrow{\sim} G_i/G_{i+1},$$

なるものを持つこと。

注意. 次が知られている ([14], Th. 9.34) : Profinite 群 G について

G は p 進解析的 $\Leftrightarrow G$ は p -uniform な指数有限部分群を含む。

N. Boston は予想 UR を研究する過程で、これを少し一般化した ([2]) :

予想 URB. 任意の完備局所 Noether 環 R で剰余体 k が有限であるものに対し、任意の連続表現 $\rho : G_{K,S} \rightarrow \mathrm{GL}_n(R)$ は像が有限である。

これはまた次の様な言い方もできる：

予想 URB'. 任意の $\bar{\rho} : G_{K,S} \rightarrow \mathrm{GL}_n(k)$ に対し、その変形理論は $G_{K,S}$ の有限商を経由する。

注意. (a) これら不分岐予想は無限次代数体や有限体上の代数函数体に対しては成立しない。前者については、岩澤理論で研究されている様に、ideal 類群が大きい pro- p 部分を含むことがしばしばある。後者については、定数体の $\widehat{\mathbb{Z}}$ -拡大のみならず、幾何学的な (i.e. 定数体の拡大を含まない) 非常に大きい不分岐拡大が存在し得る。例えば有限体上の志村曲線 (総実代数体 F 上の quaternion から作られる) は、ほとんど全ての F の有限素点 v に対し $\mathrm{PSL}_2(\mathcal{O}_{F,v})$ -型の不分岐拡大を持つ (cf. e.g. [26], [27]). これは「合同モノドロミー問題」 ([25]) の文脈で得られた非可換類体論的事実である。

(b) 一方で de Jong による次の予想と部分的な結果がある (寺杉氏も関連する結果を出している) :

予想 ([12]). X を有限体 \mathbb{F} 上の正規代数多様体とし、 p を素数 ($\neq \mathrm{char}(\mathbb{F})$) とする。 $\pi_1(X)$ を X の (ある基点に関する) 代数的基本群とし、 $\mathbb{F}_p[[t]]$ -値の連続表現 $\rho : \pi_1(X) \rightarrow \mathrm{GL}_n(\mathbb{F}_p[[t]])$ を考える。このとき $\pi_1(X)$ の幾何学的部分 $\pi_1(X \otimes_{\mathbb{F}} \mathbb{F})$ の像 $\rho(\pi_1(X \otimes_{\mathbb{F}} \mathbb{F}))$ は有限であろう。

(de Jong はもともとこの予想を Deligne の ℓ 進層についての予想との類似で考えたらしく、この節に入れるのはよくないかもしれないが、「像が有限」ということで仲間にしてしまった。この予想と Fontaine-Mazur 予想 (不分岐予想に限らず) やその他の予想との関連は意外に深いものがありそうだ。)

次に特別の場合 ($S = \phi$) として

$$\Gamma_{K,p} := \text{Gal}(\text{至る所不分岐最大 pro-}p \text{ 拡大}/K),$$

即ち K の p -類体塔の Galois 群、の表現を考える。予想 UR' より、

予想 URH. $\Gamma_{K,p}$ の任意の p 進解析的商は有限である。

例えば $\Gamma_{K,p}$ 自身は (無限群になることはある ([20]) が) p 進解析的になることは
ないだろう、ということである。

以下、これらの予想についてのいくつかの結果を紹介する。まづ Fontaine-Mazur
以前の話として、いくつか思いついたものを挙げると：

- (1) $\Gamma_{K,p}$ が無限群になる K と p が存在するか？ということすら自明ではない (類体
塔問題) わけで、これは [38]+[20] により解決された (無限群になる実例も構成され
た)。なお類体塔関係の文献については山村氏の蒐集されたものがある ([46])。
- (2) 山村氏らは特に K の判別式が小さく $\Gamma_{K,p}$ が有限のときに K の最大不分岐拡大
を決定しよう、という方向で研究を行っている ([44], [45] etc.)。
- (3) Washington の “Non- ℓ -part of the class number in a cyclotomic \mathbb{Z}_ℓ -extensions”
([41]) は、 $G_{K,\{\ell\}}$ のある商を見ているわけで、予想 UR と compatible である。

さて、予想 UR'' についての Boston の結果を紹介する：

定理 ([2]). F を代数体とし、その類数は p と素と仮定する。 ℓ は p と異なる素数と
し、 K/F を ℓ 次巡回拡大、 L/K を不分岐 pro- p 拡大であって L/F が Galois であ
るもの、とする。このとき $\text{Gal}(L/K)$ は p -uniform ではない。

(証明の概略) $G = \text{Gal}(L/K)$ とおく。これが p -uniform と仮定して、 $G = G_1 \supset G_2 \supset \dots$ をその filtration (as in (*)) とする。Schur-Zassenhaus により $\text{Gal}(L/F)$ は位数 ℓ の部分群を持つが、これを G に共役で作用させる。この作用が G/G_2 に非自明な固定点を持つことを示す (すると、この固定点は K のある p 冪次不分岐拡大に対応するが、それが F の p 冪次不分岐拡大に降りて p 類数に反する)。この作用が $= \text{id}$ ならば問題ない。もしそうでないとすると、 G は (pro-nilpotent だが) nilpotent でないから G/G_i の “nilpotency” (= どのくらい冪を取れば自明になるか、というその長さ) はどんどん大きくなって行く。Nilpotency が (固定された素数 ℓ に対し) 十分大きい有限群の ℓ 次の自己同型は 1 以外に固定点を持つ、という群論の結果 (Higman) がある (注意：この ℓ は素数でなくても (少なくとも、ある一つの pro- p 群の商たちに対しては) 成り立つと予想されているらしい)。この固定点を同型 $G_i/G_{i+1} \simeq \dots \simeq G_1/G_2$ で運んで来ればよい。Q.E.D.

この定理は G が “self-similar” の場合に一般化できる ([3]. 証明は同じ)。

Boston は予想 UR の研究の過程で次の問を発するに至った：

問題 ([2]). p を奇素数とする。 L を K の p -Hilbert 類体とし、その類数は p で割れないと仮定する。このとき不分岐 p 次巡回拡大 M/L であって M/K は Galois かつ $\text{Gal}(M/K)$ の exponent = $\text{Gal}(L/K)$ の exponent となるものが必ず存在するか？

注意. これは一般には反例がある。しかし次が知られている：

- ・ $K =$ 二次体のとき、Yes.
- ・ K の p -類体塔が無限次のとき、

予想 UR が成立 \Rightarrow Boston の問題の答は Yes.

その他、野村氏はいくつかの場合に “Yes” であることを示している ([34], [35]).

次に Hajir の結果を紹介する。

$$\rho_K := p\text{-rank}(K \text{ の ideal 類群}), \quad \nu_K := p\text{-rank}(K \text{ の単数群})$$

とおく。

定理 ([24]). $\rho_K \geq 2 + 2\sqrt{\nu_K + 1}$ ならば、

- (1) $\Gamma_{K,p}$ は p 進解析的ではない。
- (2) $\rho_{K_n} \rightarrow \infty$ (as $n \rightarrow \infty$), ここに $(K_n)_{n \geq 0}$ は $K = K_0$ の p -類体塔。

系. $\rho_K \geq 2 + 2\sqrt{\nu_K + 1}$ ならば Boston の問題の答は Yes.

注意. 上の (1) と (2) とは同値である (証明は群論; cf. [29]).

(証明の概略) $\rho_K \geq 2 + 2\sqrt{\nu_K + 1}$ という条件は $\Gamma_{K,p}$ が無限群 (i.e. p -類体塔が無限次) になるための一つの十分条件として知られていた ([20]). その証明の鍵であった、有限 p -群についての Golod-Shafarevich 不等式 (の Gaschütz-Vinberg による改良 $h^2(G) > h^1(G)/4$ が、実は p 進解析的群に対しても成立つということ ([28] etc.) がポイント (ここに $h^i := \dim_{\mathbb{F}_p} H^i(G, \mathbb{Z}/p\mathbb{Z})$).

この定理に関連して Hajir は次の問を提出している：

問 ([24]). K の p -類体塔 $(K_n)_{n \geq 0}$ が無限ならば、ある n に対し K_n は Golod-Shafarevich test をパスする (i.e. $\rho_{K_n} \geq 2 + 2\sqrt{\nu_{K_n} + 1}$ となる) か？

これが Yes ならば (上の定理により) $\Gamma_{K,p}$ 自身に対する予想 URH が成立するわけである。

次の定理は無限次不分岐 p 拡大の Galois 群はある意味で自由 pro- p 群に近い性質を持ちがちである (少なくとも、持ち得る)、ということを述べている：

定理 ([24]). 各整数 t に対し、ある代数体 K とその無限次不分岐 p 拡大 L/K とが存在して、 L/K の全ての有限次中間体 K' に対し

$$[K' : K] \cdot t \leq \rho_{K'} - 1 \leq [K' : K] \cdot (\rho_K - 1)$$

となる。

ここで右側の \leq は群論の Schreier 不等式 (cf. 次の命題) である。

命題. G を有限生成 pro- p 群とする。

- (1) H が指数 n の部分群 $\subset G$ ならば

$$h^1(H) - 1 \leq n(h^1(G) - 1).$$

- (2) G の全ての指数有限部分群 H に対し上の不等式で等号成立 $\Leftrightarrow G$ は自由 pro- p 群。

そこで Hajir は次を問うた：

問 ([24]) (a) もし $\Gamma_{K,p}$ が無限ならば $\Gamma_{K,p}$ は torsion free か？

(b) 任意の無限次不分岐 p -拡大の Galois 群には rank 2 の (離散) 自由群を埋込めるか？

これらの結果や問題を見て思うことは、 $\text{pro-}p$ 群全体の中で p 進解析的群と自由 $\text{pro-}p$ 群とはある意味で対極に位置し、 $\text{Gal}(p \text{ で激しく分岐}/K)$ は前者に、 $\text{Gal}(p \text{ で不分岐}/K)$ は後者に、それぞれ近くなりがちなのではないか？といふことです。

最後に Artin 予想との関係で Buzzard-Taylor による次の結果を紹介する：

定理 ([6]). $p \geq 5$, $p \notin S$ とし、 E を \mathbb{Q}_p の有限次拡大、

$$\rho : G_{\mathbb{Q}, S} \rightarrow \text{GL}_2(E)$$

を連続表現とする。 $\bar{\rho}$ を ρ の剰余表現とする。次を仮定する：

- (1) $\bar{\rho}$ は modular (何でもいからとにかく保型形式から来る) かつ絶対既約；
- (2) $\bar{\rho}(\text{Frob}_p)$ は二つの相異なる固有値を持つ。

このとき ρ に対する Artin 予想が成立つ (i.e. ρ は重さ 1 の保型形式から来る)。特に $\text{Im}(\rho)$ は有限である。

これは予想 UR の一つの状況証拠になっている。

証明は、 $\bar{\rho}(\text{Frob}_p)$ の二つの固有値 $\bar{\alpha}, \bar{\beta}$ に対応する重さ 2 の $\text{mod } p$ eigenforms (互いに companion form になっている) を Λ -adic eigenforms F_α, F_β に持上げる (use Wiles, Taylor, Diamond) (これらに対応する Galois 表現を重さ 1 に特殊化すると、ともに元の ρ になる)。 F_α, F_β を重さ 1 に特殊化したもの f_α, f_β は重さ 1 の overconvergent p -adic modular form であり、二つの forms

$$f = \frac{\alpha f_\alpha - \beta f_\beta}{\alpha - \beta}, \quad g = \frac{f_\alpha - f_\beta}{\alpha - \beta}$$

をうまく“貼合せて” $X_1(N)$ 上の本当の重さ 1 の保型形式を得る。

文献

- [1] V. Abrashkin, *Modular representations of the Galois group of a local field and a generalization of the Shafarevich conjecture*, Math. USSR Izv. 35(1990), 469-518
- [2] N. Boston, *Some cases of the Fontaine-Mazur conjecture*, J. Number Theory 42 (1992), 285-291
- [3] N. Boston, *Some cases of the Fontaine-Mazur conjecture II*, preprint
- [4] Ch. Breuil, *Construction de représentations p -adiques semi-stables*, Ann. Sci. Éc. Norm. Sup. 31(1998), 281-327
- [5] Ch. Breuil, *Cohomologie étale de p -torsion et cohomologie cristalline en réduction semi-stable*, Duke Math. J. 95(1998), 523-620
- [6] K. Buzzard and R. Taylor, *Companion forms and weight one forms*, preprint
- [7] R. Coleman, *Classical and overconvergent modular forms*, Invent. math. 124(1996), 215-241
- [8] R. Coleman, *p -adic Banach spaces and families of modular forms*, Invent. math. 127(1997), 417-479

- [9] R. Coleman and B. Mazur, *The Eigencurve*, in: *Galois Representations in Arithmetic Algebraic Geometry* (A. Scholl and R. Taylor, eds.), Cambridge Univ. Press, 1998, pp. 1-114
- [10] B. Conrad, *Ramified deformation problems*, in preparation
- [11] B. Conrad, F. Diamond and R. Taylor, *Modularity of certain potentially crystalline Galois representations*, preprint
- [12] A. de Jong, *A conjecture on arithmetic fundamental groups*, preprint
- [13] B. de Smit and H. Lenstra, *Explicit construction of universal deformation rings*, in: *Modular forms and Fermat's Last Theorem* (G. Cornell, J. Silverman and G. Stevens, eds.), Springer-Verlag, 1997, pp. 313-326
- [14] J. Dixon, M. du Sautoy, A. Mann and D. Segal, *Analytic pro- p Groups*, London Math. Soc. Lecture Note Ser. 157, Cambridge Univ. Press, 1991
- [15] G. Faltings, *Endlichkeitssätze für Abelsche Varietäten über Zahlkörpern*, *Invent. math.* 73(1983), 349-366
- [16] J.-M. Fontaine, *Schémas propres et lisses sur \mathbb{Z}* , in: *Proc. Indo-French Conf. on Geometry*, Hindustan Book Agency, New Dehli, 1993, pp. 43-56
- [17] J.-M. Fontaine, *Deforming semi-stable Galois representations*, in: *Elliptic curves and modular forms*, *Proc. Nat. Acad. Sci. U.S.A.* 94(1997), pp. 11138-11141
- [18] J.-M. Fontaine and G. Laffaille, *Constructions de représentations p -adiques*, *Ann. Sci. Éc. Norm. Sup.* 15(1982), 547-608
- [19] J.-M. Fontaine and B. Mazur, *Geometric Galois representations*, in: *Proc. Conf. on elliptic curves and modular forms*, Hong Kong, 1993, International Press, 1995, pp. 41-78
- [20] Golod and Shafarevich, *On class field towers*, *Izv. Acad. Nauk SSSR, Ser. Math.* 28(1964), 261-272
- [21] F. Gouvêa, *Arithmetic of p -adic modular forms*, *Lecture Notes in Math.* 1304, Springer-Verlag, 1988
- [22] F. Gouvêa and B. Mazur, *On the density of modular representations*, *AMS/IP Stud. in Adv. Math.* 7 (1998), 127-142
- [23] B. Gross, *A tameness criterion for Galois representations associated to modular forms mod p* , *Duke Math. J.* 61 (1990), 445-517
- [24] F. Hajir, *On the growth of p -class groups in p -class field towers*, *J. Alg.* 188(1997), 256-271
- [25] Y. Ihara, *The congruence monodromy problems*, *J. Math. Soc. Japan* 20(1968), 107-121
- [26] Y. Ihara, *Congruence relations and Shimura curves*, *Proc. Symp. Pure Math.* 33(1979), Part 2, 291-311
- [27] Y. Ihara, *Shimura curves over finite fields and their rational points*, to appear in: *Proc. of the Conference "Applications of Curves over Finite Fields"*, Seattle, 1997
- [28] H. Koch, *Zum Satz von Golod-Schafarewitsch*, *Math. Nachr.* 42(1969), 321-333

- [29] A. Lubotzky and A. Mann, *Powerful p -groups II. p -adic analytic groups*, J. Alg. 105(1987), 506-515
- [30] B. Mazur, *Deforming Galois representations*, in: Galois Groups over \mathbb{Q} (Y. Ihara, K. Ribet and J.-P. Serre, eds.), Springer-Verlag, 1989, pp. 385-437
- [31] B. Mazur, *An introduction to the deformation theory of Galois representations*, in: Modular forms and Fermat's Last Theorem (G. Cornell, J. Silverman and G. Stevens, eds.), Springer-Verlag, 1997, pp. 243-311
- [32] B. Mazur, *An "infinite fern" in the universal deformation space of Galois representations*, Collect. Math. 48 (1997), 155-193
- [33] H. Moon, *Finiteness results on certain mod p Galois representations*, in preparation
- [34] A. Nomura, *A remark on Boston's question concerning the existence of unramified p -extensions*, J. Number Theory 58(1996), 66-70
- [35] A. Nomura, *A remark on Boston's question concerning the existence of unramified p -extensions II*, Proc. Japan Acad. 73 (1997), 10-11
- [36] J.-P. Serre, *Sur les représentations modulaires de degré 2 de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$* , Duke Math. J. 54(1987), 179-230
- [37] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. Math. 88(1968), 492-517
- [38] I. Shafarevich, *Extensions with given ramification points*, Publ. Math. IHES 18(1964), 295-319
- [39] J. Tate, *The non-existence of certain Galois extensions of \mathbb{Q} unramified outside 2*, Contemp. Math. 174(1994), 153-156
- [40] T. Tsuji, *p -adic étale cohomology and crystalline cohomology in the semi-stable reduction case*, preprint
- [41] L. Washington, *The non- p -part of the class number in a cyclotomic \mathbb{Z}_p -extension*, Invent. math. 49(1978), 87-97
- [42] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math. 142(1995), 443-551
- [43] M. Yamagishi, *A survey of p -extensions*, to appear in: Proc. of the Conference "Class Field Theory – Its Centenary and Prospect, 1998" (K. Miyake, ed.), Math. Soc. Japan
- [44] K. Yamamura, *The maximal unramified extensions of the imaginary quadratic number fields with class number two*, J. Number Theory 60(1996), 42-50
- [45] K. Yamamura, *The maximal unramified extensions of the imaginary quadratic number fields of small conductors*, J. Théor. Nombres Bordeaux 9(1997), 405-448
- [46] K. Yamamura, 「類体塔に関する文献」

〒 060-0810 北海道大学理学部数学教室

Email: taguchi@math.sci.hokudai.ac.jp